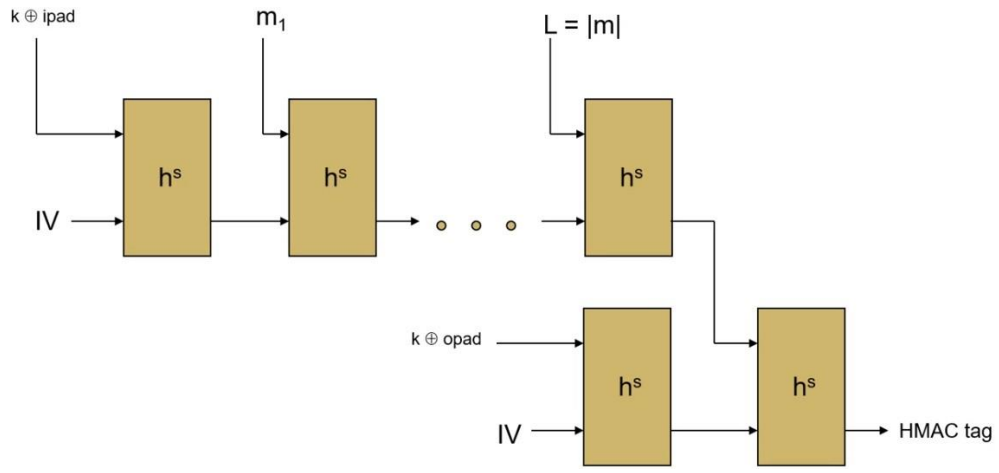
Task 8

Let H be a hash function of the merkle-damgard type, and let h be the compression function used inside H. HMAC is then simply a hash function which in practice has to be collision resistant, it can be used as MAC that we have already seen. The HMAC construction uses two constants ipad and opad, that is 0x36 and 0x5c.

Build Algorithm



Let h^s be the fixed length collision resistant hash function which for inputs of length 2n gives an outputof length n.
Then HMAC construction works as follows:

1) Key, k is chosen randomly, and IV is set to 0 ^l where l is the length of the input that fixed length hash takes.
2) We calculate k xor ipad and treat as one of the input for the first block as well as the IV as the second block.
3) The output of first block is treated as one of the inputs and the message block as the other input for the second block, this continues for each block till we get the final output.
4) The final output we get from this chain is treated as one of the input to the final block, the other input comes from another hash block which takes k xor opad and IV as its two inputs.
5) This final hash block is calculated and the output is our HMAC tag.

$$\mathbf{HMAC^s_k\,(m) = h^s_{IV}\,(k \oplus opad \,||\, h_{IV}\,(k \oplus ipad||\, m))}$$

Where, opad = 0x36 and ipad = 0x5C, both can be repeated any number of times

Proof

Theorem: Assume that H, H', h, and h' are all hash functions, where h is the fixed length collision resistant hash function and H be a derived hash function using MD transformation from h. Assume that secretly keyed H' is collision resistant and h' is a secure fixed length message auth code. Then HMAC algorithm described above is a secure message authentication code.

We already know that Discrete Log Problem is hard in Nature.

We have already proven that fixed hash used is collision Resistant in Nature.
→ We will prove the collision resistance of HMAC by contradiction

→ Let m1 and m2 be the two messages found by a polynomial time algorithm whose hash value is same, we already know that length of m1, that is |m1| and length of m2, |m2| are same, therefore |m1| = |m2|.

→ Now, since the hash computed by the last fixed hash is same for both message 1 and message 2, and since the fixed hash is collision resistant the length should be same

→ From the property that fixed hash is collision resistant m_B should also be same for both m1 and m2.

→ Therefore, the above postulate can be extended to all $m_1, m_2, \ldots\ldots m_{B-1}$.

- ➔ Hence if H^s needs to be non-collision resistant then for it the fixed hash I.e., h^s should also be non-collision resistant, which is not true.

Hence Proved by Contradiction that above construction is Collision Resistant